(12) UK Patent Application (19) GB (11) 2 372 594 (13) A

(43) Date of A Publication 28.08.2002

(21) Application No 0104670.5

(22) Date of Filing 23.02.2001

(71) Applicant(s)
Hewlett-Packard Company
(Incorporated in USA - Delaware)
3000 Hanover Street, Palo Alto, California 94304,
United States of America

(72) Inventor(s)
Siani Lynne Pearson
Richard Brown
Christopher I Dalton

(74) Agent and/or Address for Service
Richard Anthony Lawrence
Hewlett-Packard Limited, IP Section, Filton Road,
Stoke Gifford, BRISTOL, BS34 8QZ, United Kingdom

(51) INT CL[7]
G06F 1/00

(52) UK CL (Edition T)
G4A AAP

(56) Documents Cited
EP 0465016 A2 **WO 2000/054126 A1**

(58) Field of Search
UK CL (Edition S) **G4A AAP**
Online databases:WPI, EPODOC, JAPIO, INSPEC

(54) Abstract Title
Trusted computing environment

(57) *In a trusted computing environment 100, each computing device 112 to 118 holds a policy specifying* the degree to which it can trust the other devices in the environment 100. The policies are updated by an assessor 110 which receives reports from trusted components 120 in the computing devices 112 to 118 which identify the trustworthiness of the computing devices 112 to 118.

In context, a trusted device can be relied upon to work as intended and has not been tampered with or subverted to run malicious applications.

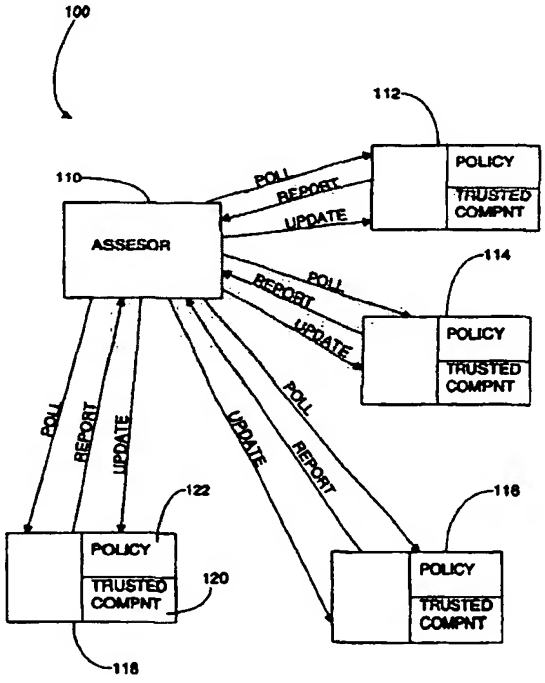


Figure 1

GB 2 372 594 A

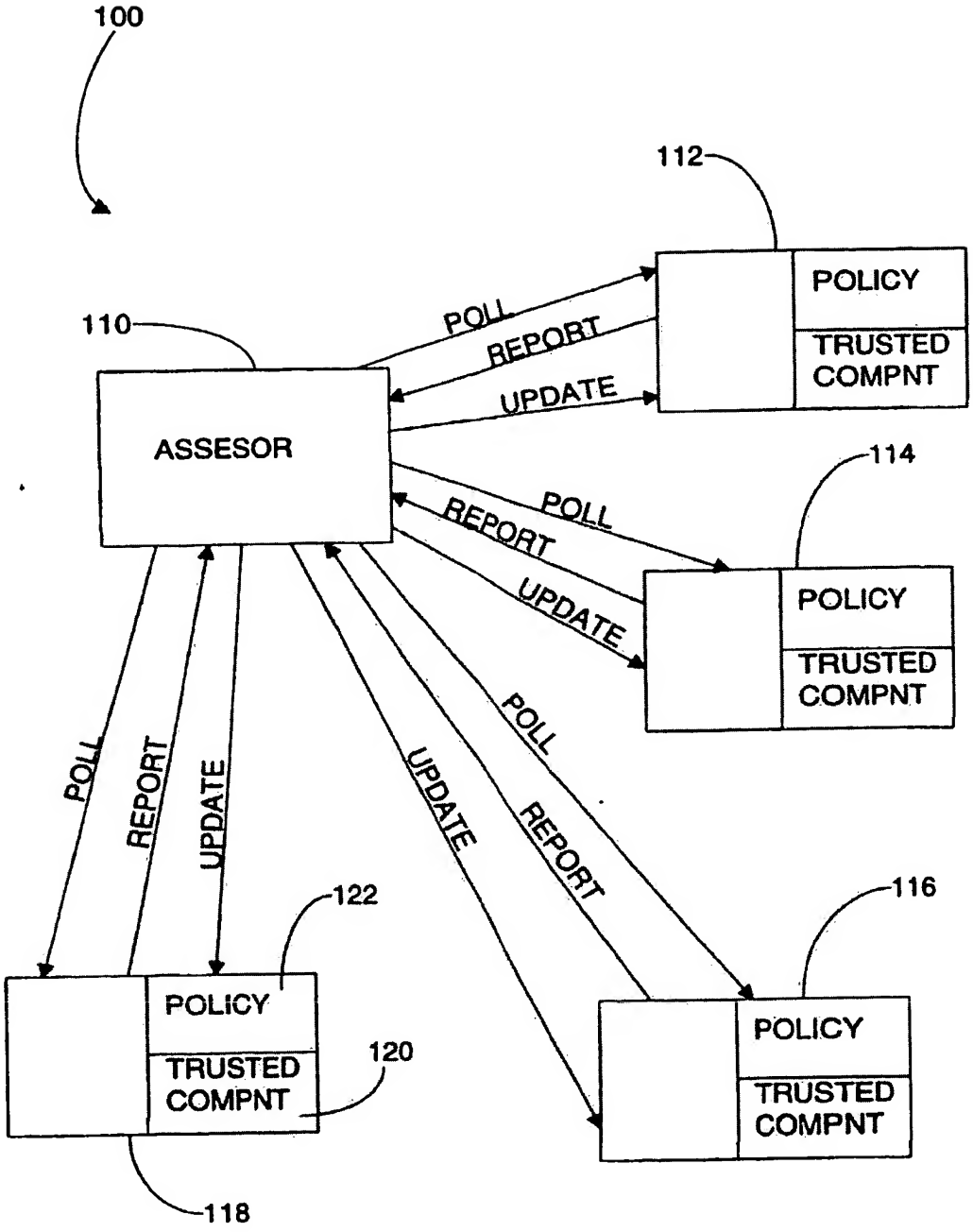

100
112
POLICY
TRUSTED COMPNT
110
POLL
REPORT
UPDATE
ASSESOR
114
POLL
REPORT
UPDATE
POLICY
TRUSTED COMPNT
POLL
REPORT
UPDATE
UPDATE
POLL
REPORT
122
116
POLICY
TRUSTED COMPNT
120
POLICY
TRUSTED COMPNT
118

Figure 1

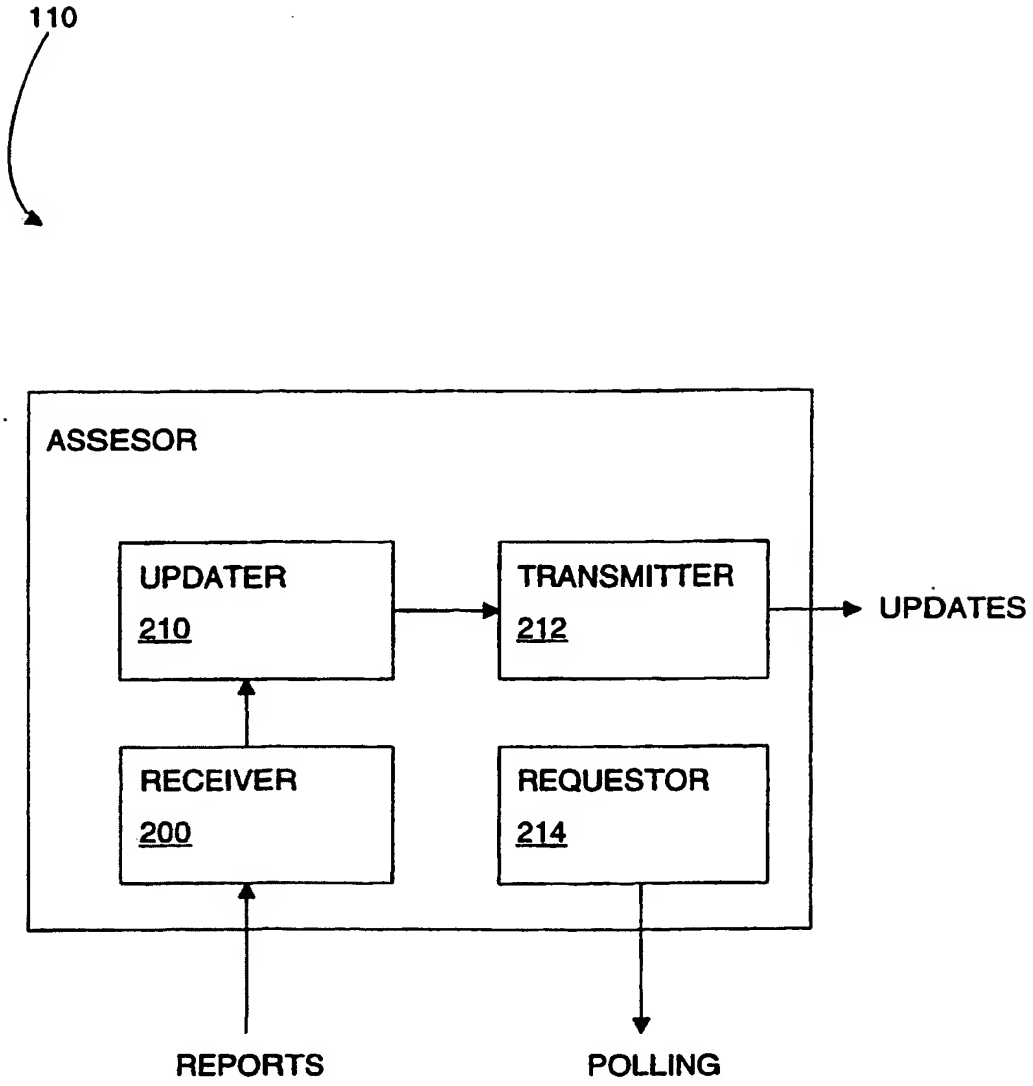

110
ASSESOR
UPDATER
210
TRANSMITTER
212
UPDATES
RECEIVER
200
REQUESTOR
214
REPORTS
POLLING

Figure 2

TRUSTED COMPUTING ENVIRONMENT

FIELD OF THE INVENTION

The invention relates establishing and/or maintaining a trusted computing environment. A first computing device can be said to regard a second computing device as trustworthy if the first computing device can expect the second computing device to operate or behave in a known manner.

BACKGROUND TO THE INVENTION

In the present context, "trust" and "trusted" are used to mean that a device or service can be relied upon to work in an intended, described or expected manner, and has not been tampered with or subverted in order to run malicious applications. A specification for trusted computing has been developed by the Trusted Computing Platform Alliance and can be found at www.trustedpc.org.

A conventional trusted computing device comprises a tamper resistant tester which can test the device to ascertain if it is trustworthy. The outcome of the test can be used within the device or reported to another computing device attempting to communicate with it. An exemplary trusted component is described in the applicants co-pending International Patent Application Publication No. PCT/GB00/00528 entitled "Trusted Computing Platform", the contents of which are incorporated by reference herein. If the outcome of the test is reported to another device, then that other device can use the report to determine a trust policy vis-a-vis the device offering the report, which controls its communication with the reporting device.

One disadvantage of a computing environment comprised of trusted computing devices of the kind mentioned above arises where a trusted computing device becomes compromised, e.g. by a virus. The trusted computing devices in the environment do not know if the other computing devices within the environment have been compromised unless they challenge

the other computing devices to verify that they have not been compromised. The challenge-verification process can consume undesirable amounts of time and/ r processing resources.

SUMMARY OF THE INVENTION

An object of the invention is the amelioration of the aforementioned disadvantage.

According to one aspect, the invention comprises a method of operating a trusted computing system, the method comprising providing an assessor to receive a report from, and pertaining to the trustworthiness of, a first computing device, and the assessor updating the trust policy of a second computing device in accordance with the report.

According to another aspect, the invention comprises an assessor for controlling a trusted computing system, the assessor comprising a receiver for receiving a report from, and pertaining to the trustworthiness of, a first computing device, an updater for updating the trust policy of a second computing device in accordance with the report, and a transmitter for transmitting the updated policy to the second computing device.

Hence, the invention can provide an efficient way of informing computing devices within an environment about the trustworthiness of other computing devices within the environment, so as to establish or maintain a trusted computing environment. In maintaining a trusted computing environment, the invention may enable a computing device to be sure of, and keep up to date with, the level of trustworthiness of other computing devices in the environment.

In one embodiment, the report contains an assessment of the trustworthiness that has been prepared by the reporting computing device itself. In another embodiment, the report provides information about the reporting computing device that is sufficient to allow the assessor to assess the trustworthiness of the reporting computing device. Preferably, the reporting computing device comprises a trusted component which evaluates the

trustworthiness of the computing device and provides the report. The trusted component is preferably resistant to tampering and capable of applying a digital signature to the report to permit authentication of the report. The reporting computing device may be triggered to provide the report in response to a certain event or any one of a number of predetermined events. For example, the reporting computing device may be triggered to report by a request from an assessor for a trustworthiness report, or by being initialised or reset, or by the occurrence of an undesirable event (e.g. the computing device being compromised by a virus).

The assessor may, subsequent to receiving a trustworthiness report, update the trust policies of more than one computing device, one of which may be the computing device that provided the trustworthiness report.

A computing device in the context of the invention may be, for example, a computer or a peripheral (such as a scanner or printer) or other device having some data processing ability.

BRIEF DESCRIPTION OF THE FIGURES

By way of example only, some embodiments of the invention will now be described by reference to the accompanying drawings in which:

Figure 1 is a block diagram of a trusted computing environment; and

Figure 2 is a block diagram of an assessor.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The trusted computing environment 100 of Figure 1 comprises an assessing computer 110, or "assessor", which acts as a service provider to the computing devices in the environment, 112, 114, 116 and 118. In practice, the environment may comprise a different number of computing devices. Each computing device has at least some capacity for processing data and therefore at least some capacity for becoming untrustworthy or

affecting the trustworthiness of other computing devices with which it communicates. In this embodiment, devices 112, 114 and 116 are networked computers and device 118 is a network printer serving devices 112, 114 and 116.

Each of the computing devices 112 to 118 comprises a trusted component and a memory 122 holding a policy. A policy allows a computing device to determine the level to which it trusts other computing devices sharing the environment.

As an example, a policy within a computing device may list the surrounding computing devices and specify the degree to which each of them is to be trusted. In order to set the degree of trust, a policy may specify that a particular computing device is to be interacted with for all purposes, selected purposes or not at all.

As a further example, a policy within a computing device may specify a list of components (either software or hardware) that are untrusted. If a computing device containing such a policy finds one or more of these components in another computing device, then it can determine accordingly the degree to which it trusts that other computing device.

Each trusted component 120 is arranged, in a known manner, to assess the trustworthiness of the computing device with which it is associated, and to report its assessment to the assessor 110. The report may contain, for example, a decision made by the trusted component as to the trustworthiness of its host computing device, or the trusted component may simply audit its host so that the report lists the components of its host. Examples of trusted components, and the monitoring of components or processes of a host, are found in the applicants co-pending International Patent Applications as follows: Publication No. PCT/GB00/02004 entitled "Data Logging in Computing Platform" filed on 25 May 2000 and Publication No. PCT/GB00/00495 entitled "Protection of the Configuration of Modules in Computing Apparatus", filed on 15 February 2000, the contents of which are incorporated by reference.

The trusted component 120 can be arranged to be triggered to report by any of a number of events. For example, the report can be triggered by a request for a report received from the assessor 110, initialisation or resetting of the host computing device, or by some undesirable event (e.g. detection of the computing device being compromised by a known virus or the loading or addition of components unrecognised by the trusted component). Alternatively, the trusted component 120 can be arranged to make periodic reports to the assessor.

To maintain security, the trusted component 120 and the memory 122 holding the policy are incorporated in the corresponding computing device in such a manner that the trusted component 120 can perform its assessments on the computing device and yet the computing device is unable to modify the operation of the trusted component or the content of the policy. The memory 122 is arranged to accept updates to the policy that are certified by containing the digital signature of the assessor 110. Similarly, the trusted component is arranged to certify its outgoing reports with a digital signature which the assessor 110 can verify. The memory 122 containing the policy may be integrated with the trusted component 120.

As shown in Figure 2, the assessor 110 comprises a receiver 200, an updater 210, a transmitter 212 and a requestor 214. In response to being polled by the requestor 214, the receiver 200 receives the reports from the trusted components (which contain, for example, decisions on trustworthiness or component inventories), the updater 210 updates the computing devices' policies as necessary and the transmitter 212 disseminates the updated policies. Clearly it is desirable that the assessor 110 or at least relevant functions thereof are also trusted.

In the present embodiment, the assessor polls the trusted components within the computing devices 112 to 118 for trustworthiness reports. Consider the case where printer 118 has been contaminated by a virus. The report from this device alerts the assessor 110 to this fact and the assessor 110 responds by transmitting updated policies to the computing devices 112 to 118. The extent to which an updated policy curtails the extent to which the

computing device hosting the policy interacts with the affected device 118 depends on the relationship between the two computing devices. In this example, the policy of device 116 is updated to reflect that it can only send urgent print requests to printer 118 and the policies of devices 112 and 114 are updated to reflect that they are not to interact with the printer 118 or, due the continuing potential for it to be compromised by printer 118, computing device 116.

Due to the invention, a trusted computing network or environment can be established or maintained without a computing device being required to directly challenge the trustworthiness of another device when it is required to communicate with that device.

CLAIMS

1. A method of operating a trusted computing system, the method comprising an assessor receiving a report from, and pertaining to the trustworthiness of, a first computing device, and the assessor updating the trust policy of a second computing device in accordance with the report.

2. A method according to claim 1, wherein the assessor updates the trust policies of multiple computing devices in accordance with the report.

3. A method according to claim 1 or 2, wherein the assessor updates policies by assessing the trustworthiness of the first computing device on the basis of information about the first computing device in the report.

4. A method according to claim 1 or 2, wherein the assessor updates policies on the basis of an assessment of the trustworthiness of the first computing device contained in the report.

5. A method according to any one of claims 1 to 4, wherein the assessor requests the first computing device to make the report.

6. A method according to any one of claims 1 to 4, wherein the first computing device is caused to report by being started-up or reset, or by an undesirable event occurring.

7. A method according to any one of claims 1 to 4, wherein the first computing device is caused to report periodically.

8. An assessor for controlling a trusted computing system, the assessor comprising a receiver for receiving a report from, and pertaining to the trustworthiness of, a first computing device, an updater for updating the trust policy of a second computing device in accordance with the report, and a transmitter for transmitting the updated policy to the second computing device.

9. An assessor according to claim 8, wherein the updater is arranged to update the trust policies of multiple computing devices in accordance with the report and the transmitter is arranged to transmit the updated policies to the multiple computing devices.

10. An assessor according to claim 8 or 9, wherein the updater updates policies by assessing the trustworthiness of the first computing device on the basis of information about the first computing device in the report.

11. An assessor according to claim 8 or 9, wherein the updater updates policies on the basis of an assessment of the trustworthiness of the first computing device contained in the report.

12. An assessor according to any one of claims 8 to 11 further comprising a requestor, for requesting the report from the first computing device.

13. A system comprising an assessor for controlling a trusted computing system, the assessor comprising a receiver for receiving a report from, and pertaining to the trustworthiness of, a first computing device, an updater for updating the trust policy of a second computing device in accordance with the report, and a transmitter for transmitting the updated policy to the second computing device, and the system further comprising first and second computing devices, wherein at least the first computing device comprises a reporter for sending a trustworthiness report to the assessor and at least the second computing device comprises a memory maintaining a trust policy such that the trust policy is modifiable by the transmitter.

INVESTOR IN PEOPLE

Application No:	GB 0104670.5	**Examiner:**	Sue Willcox
Claims searched:	1, 8, 13	**Date of search:**	26 November 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): G4A AAP

Int Cl (Ed.7):

Other: Online databases: WPI, EPODOC, JAPIO, INSPEC

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	EP 0465016 A2	(DIGITAL EQUIPMENT CORP) - see particularly col. 11, lines 15 - 35	1, 8, 13 at least
X	WO 00/54126 A1	(HEWLETT-PACKARD) - see abstract	1, 8, 13 at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the *declared priority* date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

(12) UK Patent Application (19) GB (11) 2 372 595 (13) A

(43) Date of A Publication 28.08.2002

(21) Application No 0104673.9

(22) Date of Filing 23.02.2001

(71) Applicant(s)
Hewlett-Packard Company
(Incorporated in USA - Delaware)
3000 Hanover Street, Palo Alto, California 94304,
United States of America

(72) Inventor(s)
Siani Lynne Pearson
Graeme John Proudler

(74) Agent and/or Address for Service
Richard Anthony Lawrence
Hewlett-Packard Limited, IP Section, Filton Road,
Stoke Gifford, BRISTOL, BS34 8QZ, United Kingdom

(51) INT CL[7]
G06F 1/00

(52) UK CL (Edition T)
G4A AAP

(56) Documents Cited
EP 1056014 A1 EP 1030237 A1
EP 0465016 A2 WO 2001/023980 A1
WO1998/040809 A2
"BUILDING A FOUNDATION OF TRUST IN THE PC", TCPA, JAN. 2000,WWW.TRUSTEDPC.ORG/HOME/HOME.HTM.

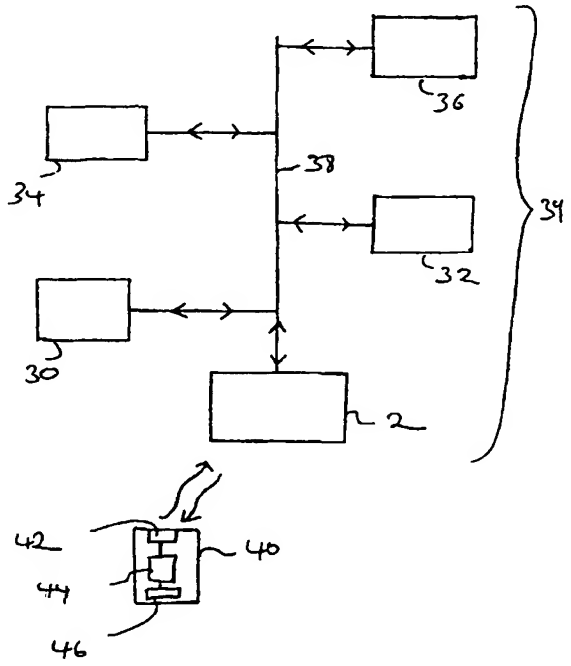
(58) Field of Search
UK CL (Edition S) G4A AAP
INT CL[7] G06F 1/00
ONLINE DATABASES: WPI, EPODOC, JAPIO, INSPEC, INTERNET.

(54) Abstract Title

Method of and apparatus for ascertaining the status of a data processing environment.

(57) In order to facilitate a user's ability to trust a computing environment, a trusted computing device 2 is arranged to challenge other devices in the computing environment and to record a log of the facilities available within the computing environment and an indication of whether those facilities are trustworthy. A new user 40 entering the computing environment can obtain the log from the trusted computing device in order to ascertain the status of the environment. Alternatively any device can hold data concerning platforms in its vicinity and its operation can be authenticated by the trusted device.

Fig 2



GB 2 372 595 A

Fig 1

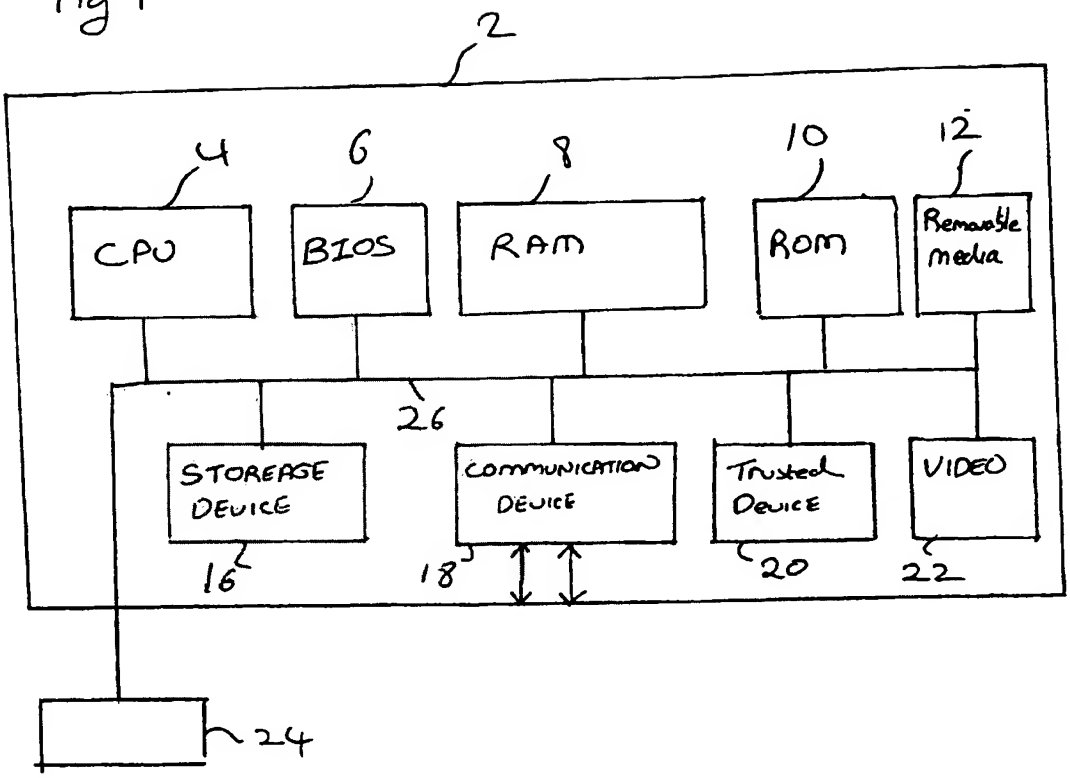

2
4
6
8
10
12
CPU
BIOS
RAM
ROM
Removable media
26
STOREAGE DEVICE
COMMUNICATION DEVICE
Trusted Device
VIDEO
16
18
20
22
24

Fig 2

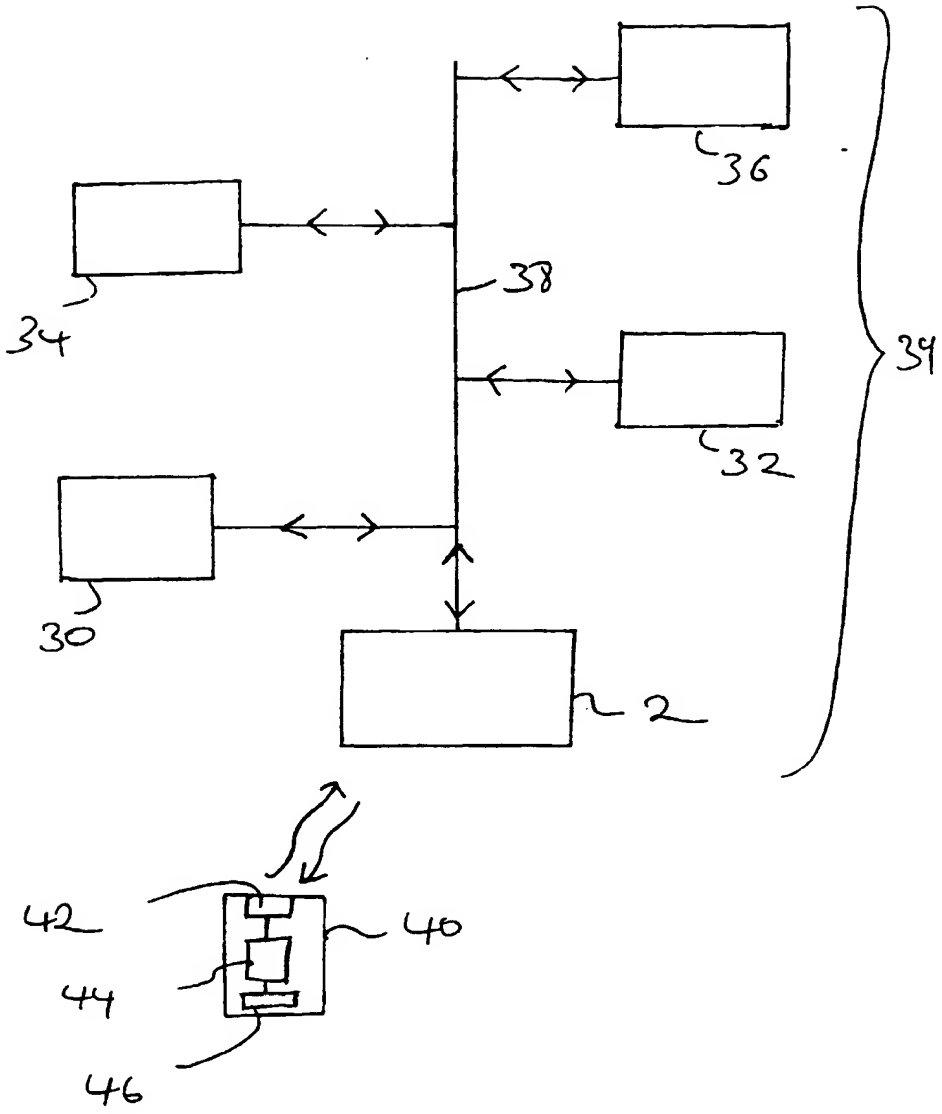


Fig 3

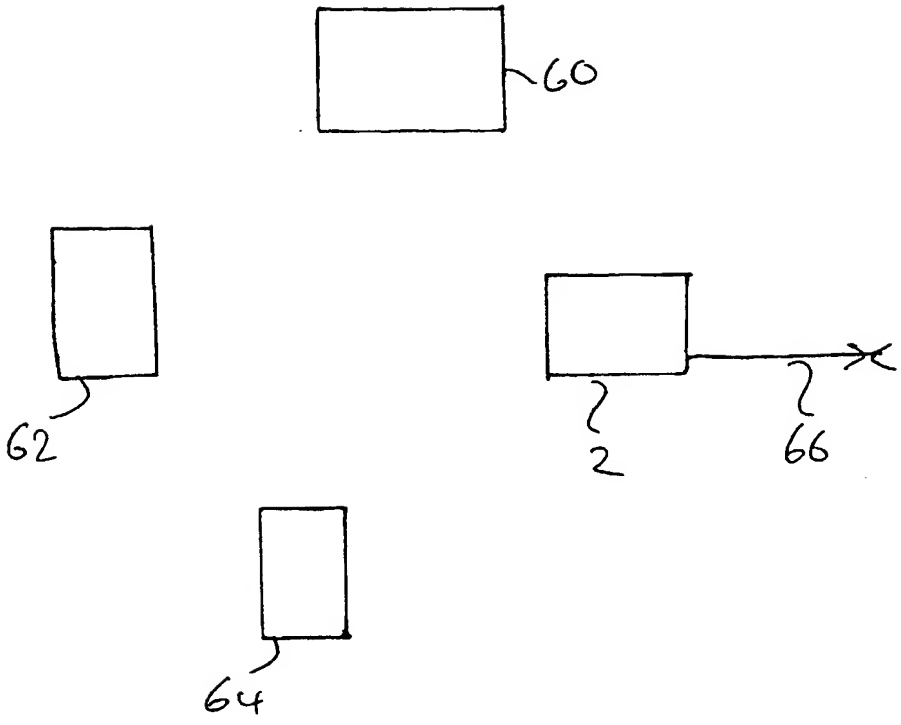


Fig 4

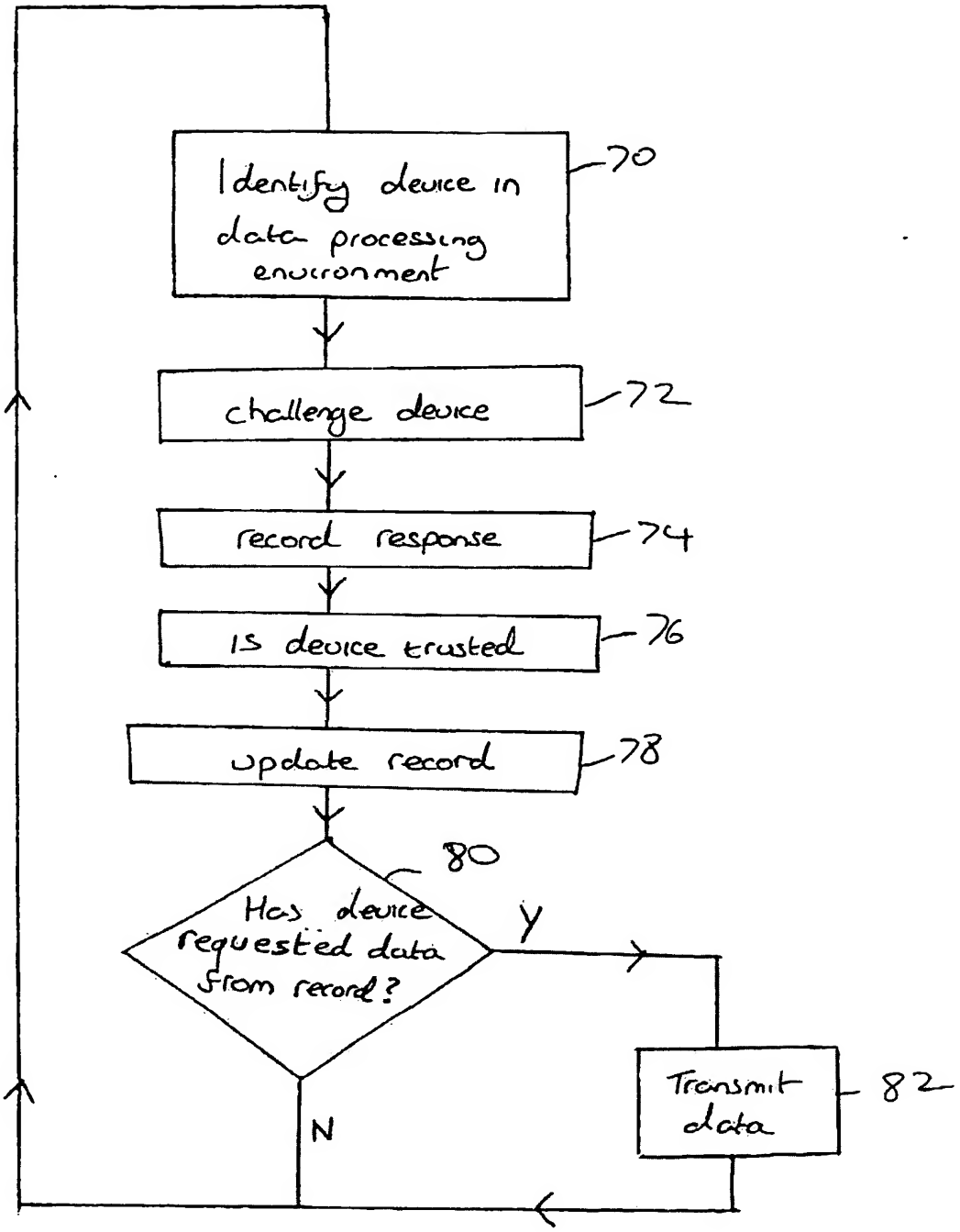

Identify device in data processing environment
70
challenge device
72
record response
74
Is device trusted
76
update record
78
Has device requested data from record?
80
Y
N
Transmit data
82

Fig 5

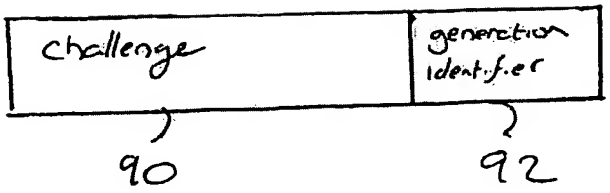
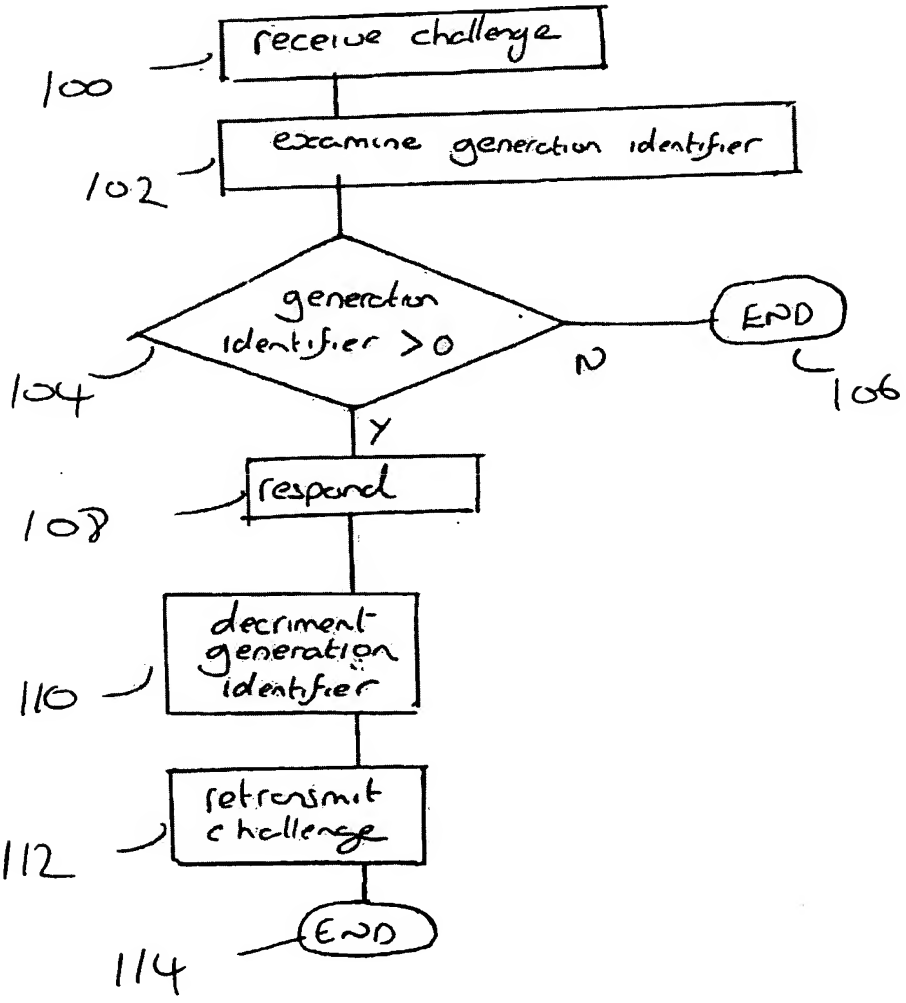

challenge
generation identifier
90
92

Fig 6


receive challenge
100
examine generation identifier
102
generation identifier > 0
104
N
END
106
Y
respond
108
decriment generation identifier
110
retransmit challenge
112
END
114

METHOD OF AND APPARATUS FOR ASCERTAINING THE STATUS OF A DATA PROCESSING ENVIRONMENT

Technical Field

The present invention relates to a method of and apparatus for determining status of a data processing environment. The information concerning the status of the environment may include an indication of what devices are operating within the environment, what facilities they offer and whether the devices can be trusted.

Background Art

The issues of security and ease of use of a computing platform are often in conflict. For commercial applications, a client computing platform typically operates in an environment where its behaviour is vulnerable to modification. Such modification can be made by local or remote entities. This has given rise to concerns, especially in the field of e-commerce, that transactions conducted on a computer might be subject to some form of misdemeanour, such as theft of credit card details. These perceived insecurities may limit the willingness of users to undertake e-commerce transactions on either local or remote computer systems.

There are existing security applications, such as virus checkers and fire walls which can be installed in computer systems in order to limit their vulnerability to viruses or to malicious users seeking to take control of the machine remotely. However, these security applications execute on computing platforms under the assumption that the platform is operating as intended and that the platform itself will not subvert the processes used by these applications.

Users engaging in communication with a remote or unfamiliar data processing environment may nevertheless be concerned about the security of that environment as a whole rather than just the security of the computing device with which they have made initial contact. Thus users seek reassurance that the computing environment can be trusted.

As used herein, the word "trust" is used to mean that something can be trusted, in the sense that it is working in the way that it is intended and expected to work and is not or has not been tampered with in order to run malicious operations.

Disclosure of the Invention

According to a first aspect of the present invention, there is provided an apparatus for ascertaining the status of a data processing environment, comprising at least one trusted computing device which is arranged to challenge other devices within a data processing environment, to keep a record of the responses and to make the record available.

It is thus possible to use a trusted computing device to keep an audit of the status of a data processing network. The trusted device can challenge new devices as and when it discovers them within the data processing environment and can also re-challenge known devices every now and again in order to ascertain that they are functioning correctly. In such a challenge, a trusted computing device extracts from the challenged device a response to the challenge. Preferably the challenged device enters into a predefined challenge - response protocol, such as a TCPA challenge - response protocol in order to return trusted integrity and identity information about the challenged device. Thus the response may include information which can be analysed to determine the integrity of the challenged device, such as at least one integrity metric. The trusted device, upon receiving the response, extracts the integrity information from the response and compares it with an authenticated metric for the challenged device. As a result of the comparison, the trusted device can indicate whether the challenged device can be trusted or not. By keeping a record of the time that a device is challenged, the response received from the device and the result of the comparison of the integrity metrics, the trusted computing device can maintain a log of the status of the data processing environment.

The integrity information would normally include a cryptographic representation of at least one platform component. This may, for example, include the BIOS, operating system or an application. Preferably the integrity information is of the form described in the TCPA specification (www.trustedpc.org) and has been measured and stored in the form described in the TCPA specification.

Advantageously other devices within the data processing environment can also issue challenges. The responses to those challenges and conclusions concerning trustworthiness can be recorded by the at least one trusted computing device. An indication of which devices acted as challenger and challengee can also be recorded, together with an indication of whether the challenger is itself established as trustworthy.

Preferably the challenges to known devices are made on a periodic basis in order to maintain an up to date record of the integrity of the data processing environment. However, additional challenges may also be made when a device attempts to perform an operation within the environment which requires that device to be trusted. Thus attempts to read, create or modify sensitive data, whether this data be user data, application data or system data (as defined by a system administrator) may require re-authentication of the trustworthiness of the device before it is enabled to have such access.

Advantageously the record held by the trusted device includes historical data representing the status of the network. Such data may be of use during investigations of system performance in order to indicate when a data processing environment could be regarded as trustworthy and/or what devices or processes may have entered or been executed in that environment. This information may be of use to administrators or investigators when seeking data concerning fraudulent transactions or attempts to subvert the operation of one or more components within the system.

In order to maintain a record of the devices within the computing environment, the trusted computing device needs to ascertain what devices are there. It can do this by sending query messages into the environment. The queries may be specific, that is directed to a known device in order to ascertain that it is still there and functioning. However, the queries may also be more general. Thus, for example, the trusted computing device could issue a query to a class of devices, for example printers, to identify what printers are available within the data processing environment. Such a query could then be repeated for a different class of device in order to build up a picture of the data processing environment. Alternatively, the trusted computing device could issue a general query asking devices to respond by identifying themselves, and optionally their functionality and/or integrity metrics. Advantageously the query also includes a generation identifier such that the age of the query can be ascertained by devices receiving the query. In this context, age can be

measured in either or both the temporal sense or the number of retransmissions that the message has undergone. It is particularly desirable to limit the number of retransmissions that the query message may undergo as in extreme cases the message could propagate out of a local computing environment via, for example, a communications link to the internet and then computing devices receiving that query message could then attempt to respond. If this were the case, the trusted computing device could be overwhelmed by responses from computers which do not really constitute part of the data processing environment but which nevertheless have managed to receive the query message.

The trusted computing device can also listen to data communications on a network or between devices local to it in order to ascertain what devices are operating. The need to listen for devices entering and leaving the data processing network is likely to become more prevalent with the general increase in the number of portable computing devices and the ease at which these can enter or leave data processing environments as a result of the increase in wireless communication links to join computing devices, for example Blue Tooth.

When a user with a portable computing device or a remote user using a telecommunications link wishes to interact with a data processing environment, the user may seek to challenge the integrity of that environment. The functionality of the user's computing device and/or the communications bandwidth between the user's device and the data processing network may limit the ability of the user to make individual challenges to each device in the data processing environment. However, the user may still seek confirmation that the data processing environment is secure, or at least an indication of the trust which he should place in that data processing environment (for a user may still decide to use a data processing environment even if that data processing environment is not deemed to be trustworthy - this is the user's choice depending on the type of transaction that the user wishes to undertake and the urgency ascribed to that transaction). With the present invention, a user does not need to make individual challenges to each device, but instead can seek this data from the trusted computing device. The user can trust the data from the trusted computing device because the user can challenge the trusted computing device and analyse the response to the challenge, comparing the integrity metrics received from the trusted computing device with those which are certificated as being the correct

metrics, thereby enabling the user to determine whether the trusted computing device is itself trustworthy. The user can also determin what facilities are available in the computing environment.

According to a second aspect of the present invention, there is provided a computing device including a communications device and a data processor wherein the data processor is arranged to establish communication with a trusted computing device via the communication device, to receive at least part of the record of responses and to establish from an internal rules base whether the data processing environment is trustworthy enough to enable a class of transaction or task to be carried out in that environment.

According to a third aspect of the present invention, there is provided a computing device including a communications device and a data processor, wherein the computing device uses the communication device to establish communication with at least one device within a data processing system, and in which the data processor is arranged to identify challenges from at least one trusted computing device, to apply response rules to the challenge and, if a response is indicated, to respond to the challenge in accordance with the rules.

Advantageously, when the computing device receives a challenge from the trusted device it examines a generation identifier in order to see whether the message is still valid. The generation identifier may be a skip number. Thus, each time the challenge is retransmitted the skip number is modified, and every time a device receives a challenge, it checks the skip number to see if the challenge is valid. For convenience, the trusted computing device may set the skip number to an integer value greater than zero, and the skip number may be decremented at each retransmission. Any device receiving a challenge with a skip number of zero ignores the challenge and does not retransmit the challenge. This prevents the challenge from propagating too widely.

According to a fourth aspect of the present invention, there is provided a method of ascertaining the status of the data processing environment, the method comprising the steps of using a trusted computing device to challenge other devices within a data processing environment, keeping a record of the responses made to the challenges and making the record available.

Preferably the trusted computing device will itself respond to a challenge such that the integrity of the trusted computing device can be verified by the device which challenged it.

According to a further aspect of the present invention, there is provided a method of conducting a transaction in a data processing environment comprising a user device and at least a trusted computing device each having respective communications capabilities, wherein the trusted computing device keeps a record of computing devices that it has identified within the data processing environment, and wherein the user device is arranged to establish communications with the trusted computing device, to receive therefrom at least a portion of the record of computing devices within the data processing environment, and to analyse the record to establish what facilities the user device may access.

Preferably the user device further analyses the record in accordance with a set of security rules contained therein to determine what level of trust the user device can place on the integrity of the data processing environment.

It is thus possible to provide a trusted record of the status and trustworthiness of devices within a data processing network such that a computing device can be spared the task of challenging each device in the computer network in order to ascertain its trustworthiness, but instead can obtain a record of the challenges from a trusted computing device.

Brief Description of the Drawings

The present invention will further be described, by way of example, with reference to the accompanying drawings, in which:

Figure 1 is a schematic diagram illustrating the functional components within a trusted computing device;

Figure 2 schematically illustrates the structure of a first data processing environment including a trusted computing device;

Figure 3 schematically illustrates a second data processing environment including a trusted computing device;

Figure 4 is a flow chart illustrating the steps undertaken by a trusted computing device in order to maintain a record of the local data processing environment;

Figure 5 illustrates the data layout of the challenge issued by the trusted computing device; and

Figure 6 is a flow chart illustrating the response of a device in the data processing environment upon receiving a challenge.

Best Mode for Carrying Out the Invention

Many of the concepts underlying trusted computing have already been published. In particular, a specification concerning the functionality of a trusted computing environment has been published by the "trusted computing platform alliance" on their web site at www.trustedpc.org. A trusted computing device of this general type is described in the applicant's co-pending International Patent Application Publication No. PCT/GB00/00528 entitled "Trusted Computing Platform", filed on 15 February 2000, the contents of which are incorporated by reference herein.

In essence, it is desirable to ensure that a computer is trustworthy. In broad terms, this can be achieved by attaching to or embedding in a computer a trusted physical device whose function in relation to that computer is to obtain measurements of data from the computer which provides an integrity metric of the computer platform. The identity of the computing platform and the integrity metric are compared with expected values that are provided by a trusted party whose role it is to vouch for the trustworthiness of the platform. If the identities and metrics match, then there is a strong implication that the platform is operating correctly. The trusted physical device is normally provided as a tamper evident component such that attempts to interfere with its operation will result in its performance being modified when it is next used.

A trusted platform is illustrated in Figure 1. The platform 2 includes a central processing unit 4, which is in communication with BIOS memory 6, Random Access Memory 8, Read Only Memory 10, a removable data storage device 12, an internal mass storage device 16, at least one communications device 18, a trusted device 20, a video board and associated display 22, and a user input device such as a keyboard 24, via a data bus 26. In a

conventional computing device, at power up or reset the CPU initially reads instructions from the BIOS 6. In the early days of computing the BIOS memory which is non-volatile was hard wired and therefore it was not possible to modify its contents. However, with the development of EEPROM it has become possible to modify the BIOS of a computer system. In a trusted computing environment, the boot-up sequence is modified such that the CPU first looks to the trusted device 20 for instructions after reset or power-up. The trusted device 20, having gained initial control of the CPU, then enables the CPU to execute the BIOS program held in the BIOS memory 6. The trusted device can investigate integrity metrics in the BIOS program, such as check sums for the whole or specific part of the BIOS or data at specific addresses in order to determine that the BIOS has not been interfered with or modified. It can compare these values against values certified as being correct by the trusted party. The BIOS 6 may advantageously be contained within the trusted device, thereby ensuring that the BIOS builds the correct environment for the operating system. The trusted device can also, through its interaction with the BIOS, enforce the operation of various security policies. After the BIOS has been loaded, the CPU can then seek to load its operating system from the storage device 16. Once again, the trusted device 20 can challenge the operating system to extract integrity metrics from it and to compare these with metrics provided by the trusted party. Thus, as the system builds up from power-up or reboot the BIOS is first confirmed as trustworthy, and once this has been established tests are made to see that the operating system is trustworthy, and once this has been established further tests may be made to ensure that applications executing on the trusted computer platform are also trustworthy. The trusted computing platform need not be a general purpose PC wherein applications are loaded from the mass storage device 16 to the random access memory 8, and indeed the trusted device could be an embedded system. In which case, it is likely that application data may also be held in read-only memory 10. The trusted computing device may have a reader 12 for removable media, such as floppy discs, or for interfacing with the smart cards which may be used to help authenticate the identity of a local user who seeks to operate the trusted computing device 2 via its keyboard 24. An interface to the local user is provided via the keyboard 24 and the video display 22, as is well known. The trusted computing device 2 also has a communications device 18 which may support one or more of direct connection with a

local area or wide area network, wireless communications, infrared or ultrasonic communication and/or communications with a telecommunication network via a data link.

As shown in Figure 2, the trusted computing device 2 can be a component within a relatively well defined network. Thus other devices such as a printer 30, a scanner 32, and user devices 34 and 36. Each device is connected via a local area network 38. In this environment, the communications medium between devices is well defined and a number of devices on the network can be expected to change only relatively slowly.

A user's device 40, for example in the form of a personal digital assistant can establish communications with the trusted computing device 2 via the communications device 18 of the trusted computing device 2 and also a communications port 42 of the personal digital assistant. The personal digital assistant 40 also includes a central processing unit 44 and a memory 46 holding a set of security rules which the processor 44 uses to decide whether or not it should regard the data processing environment as trustworthy or not.

In use, the trusted computing device 2 challenges the devices 30 to 36 in its computing environment 38 and keeps a record of their responses, including integrity metrics, which enables it to work out whether the devices 30 to 36 can be trusted, that is that they are behaving in an expected manner and have not been subverted by external or malicious processes. The trusted device 2 keeps a record of the results of the challenges in its memory 8 and on the mass storage device 16 (see Figure 1).

When the user's device wishes to use the facilities available of the computing network 39, it establishes communication with the trusted computing device 2, and challenges it in order to assure itself that the trusted computing device is a trusted computing device and not some rogue device masquerading or spoofing as a trusted computing device. Once the user device 40 has completed the challenge and compared the integrity metric retrieved from the trusted computing device with an expected integrity metric as certified with a trusted authority, the user device 40 may then query the trusted computing device 2 in order to obtain a list of the devices available in the local computing area, the functions that they can perform and whether or not they are trustworthy. Having received this data, the user device 40 then applies the security rules held in the memory 46 in order to determine whether, in accordance with those rules which themselves are defined either by the device

owner, administrator or some other person given the rights to modify those rules, whether the local computing environment is trustworthy. If so, the user is informed. Alternatively, the user may be informed if the computing environment is not trustworthy. The user may also be informed which classes of transactions should or should not be undertaken in this environment.

Not all computing environments are as well defined as that shown in Figure 2. Companies may wish to offer computing facilities in publicly accessible environments where it can be expected that most users will establish local wireless communications with some form of gateway or server whilst they are in the environment. Thus, as shown in Figure 3 a trusted computing device 2 may be situated in an environment with a display device 60. Users 62 and 64 having portable computing devices such as personal digital assistants or palm top computers may enter the computing area around the devices 2 and 60 and may establish wireless communications with the trusted computing device 2 in order to enquire what facilities are available in the computing area. The computing device 2 may then inform the devices 62 and 64 about the existence of the display device 60 such that these devices can then interface with it for example to display data which they are not capable of displaying on their own inbuilt display devices. The trusted computing device 2 may also seek to inform each mobile device 62 and 64 about the presence of the other. The trusted computing device may also provide details about access to a telecommunications network 66.

Figure 4 schematically illustrates a sequence by which the trusted computing device 2 can maintain its record of devices in the data processing environment. Starting at step 70, the trusted computing device 2 listens to data traffic in the computing environment to identify the presence of any new devices. Once the device has been identified, control is passed to step 72 where the trusted computing devices issues a challenge to the new device. Any response made by that device is recorded at step 74, together with the time at which the response was received and then control is passed to step 76 where an analysis of any integrity metric returned by the challenged device is made in order to ascertain whether the device is trustworthy. The result of the analysis is recorded at step 78. The challenged device, or indeed any other device on the network may issue a request to the trusted device to seek information from the record, a test for any such request is made at step 80. If a

request has been received, that data is transmitted at step 82, otherwise control is returned to step 70 where the integrity check can be repeated.

In a modification of the flow chart showing in Figure 4, steps 70 and 72 may be replaced by a single broadcast challenge. Such a broadcast challenge is schematically shown in Figure 5. The broadcast challenge comprises two parts, the first being the challenge message 90 and the second part being a generation identifier 92.

Devices receiving the challenge shown in Figure 5 may execute the procedure shown in Figure 6. The procedure starts at step 100 where the device receives the challenge. Control is then passed to step 102 where the generation identifier is examined. In a preferred embodiment of the invention, the generation identifier is set to a positive integer number which controls the number of retransmissions which the challenge may undergo. Each time the challenge is retransmitted, the generation identifier is decremented by the device that retransmits the challenge. Thus, once the generation identifier reaches zero the challenge has become "old" and is no longer valid. At step 104 a test is made to see if the generation identifier is greater than zero, if not, control is passed to step 106 where the challenge handling routine is terminated. If the generation identifier is greater than zero control is passed to step 108 where, if the device is programmed to participate in these challenges, it responds to the challenge. From step 108 control is passed to step 110 where the challenge identifier is decremented and then to step 112 where the challenge is retransmitted with the decremented generation identifier. Control is then passed to step 114 which represents the end of this routine.

It is thus possible to provide a measure of the integrity and facilities available within a local, and possibly varying data processing network.

CLAIMS

1. An apparatus for ascertaining the status of a data processing environment, comprising at least one trusted computing device which is arranged to challenge other devices within a data processing environment, to keep a record of the response and to make the record available.

2. An apparatus as claimed in claim 1, in which the trusted computing device is arranged to make periodic challenges to the other devices in order to maintain the accuracy of the record.

3. An apparatus as claimed in claim 1 or 2, in which the record indicates the historical status of the data processing environment.

4. An apparatus as claimed in any one of the preceding claims, in which the at least one trusted computing device is arranged to listen to communications within the data processing environment so as to identify the presence of new devices.

5. An apparatus as claimed in any one of the preceding claims, in which the record includes data identifying the type of devices in the data processing environment.

6. An apparatus as claimed in any one of the preceding claims, in which the trusted computing device is arranged to analyse the responses it receives in order to determine if a given device in the data processing environment is trustworthy.

7. An apparatus as claimed in claim 6, in which the record indicates whether a device has been judged as trustworthy by the trusted computing device.

8. An apparatus as claimed in any one of the preceding claims, in which the at least one trusted computing device acts as a gateway to the data processing environment.

9. An apparatus as claimed in any one of the preceding claims, in which the at least one trusted computing device is a server.

10. An apparatus as claimed in any one of the preceding claims in which the at least one trusted computing device transmits a challenge which includes a generation identifier which enables devices receiving the challenge to identify whether the challenge is valid.

11. An apparatus as claimed in any one of the preceding claims, wherein the at least one trusted device is arranged to act as a proxy gateway to facilitate the exchange of data between devices in the data processing environment.

12. A computing device including a communication device and a data processor, wherein the data processor is arranged to establish communication with a trusted computing device via the communication device, to receive at least part of the record of responses and to establish from an internal rules base whether the data processing environment is trustworthy enough to enable a class of transaction or task to be carried out in that environment.

13. A computing device including a communication device and a data processor, wherein the computing device uses the communication device to establish communication with at least one device within a data processing system, and in which the data processor is arranged to identify challenges from at least one trusted computing device, to apply response rules to the challenge and, if a response indicated, to respond to the challenge in accordance with the rules.

14. A computing device as claimed in claim 13, in which the computing device is arranged to search for a generation identifier within the challenge, to apply response rules to the generation identifier to see if the challenge is still valid, and if it is not to disregard the challenge.

15. A computing device as claimed in claim 14, in which the computing device retransmits the challenge with a modified generation identifier if the challenge is valid.

16. A method of ascertaining the status of a data processing environment, comprising the steps of using a trusted computing device to challenge other devices within a data processing environment, keeping a record of responses made to the challenges and making the record available.

17. A method as claimed in claim 16, in which the trusted computing device is arranged to continue to challenge the devices in the data processing environment so as to maintain an evolving record of the status of the data processing environment.

18. A method as claimed in claim 16 or 17, in which the record includes a historical status of the data processing environment.

19. A method as claimed in any one of the claims 16 to 18, in which the at least one trusted computing device is arranged to listen to communications within the data processing environment so as to identify the presence of new devices.

20. A method as claimed in any one of claims 16 to 19, in which the challenge generated by the trusted device includes a generation identifier such that any device receiving the challenge can examine the generation identifier in order to establish whether the challenge is directly received from the trusted computing device or whether it has been retransmitted.

21. A method of conducting a transaction in a data processing environment comprising a user device and at least a trusted computing device each having respective communication capabilities wherein the trusted computing device keeps a record of computing devices that it has identified within the data processing environment, and where in the user device is arranged to establish communications with the trusted computing device, to receive therefrom at least a portion of the record of computing devices within the data processing environment, and to analyse the record to establish what facilitates the user device may access.

22. A method of conducting a transaction as claimed in claim 21, wherein the user device further analyses the record in accordance with a set of security rules to determine what level of trust can be placed on the integrity of the data processing environment.

Application No: GB 0104673.9
Claims searched: 1, 12, 13, 16, 21

Examiner: Matthew Males
Date of search: 21 November 2001

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.S): G4A AAP

Int Cl (Ed.7): G06F 1/00

Other: Online databases: WPI, EPODOC, JAPIO, INSPEC, Internet

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X	EP 1056014 A1	HEWLETT-PACKARD LTD. - whole document but see abstract.	1, 16 at least
X	EP 1030237 A1	HEWLETT-PACKARD LTD. - whole document but see abstract.	1, 16 at least
X	EP 0465016 A2	DIGITAL EQUIPMENT CORP. - whole document but see abstract, column 8, line 27 onward and Figures 3, 4A & 4B.	1, 13, 16 at least
X, E	WO 01/23980 A1	HEWLETT-PACKARD LTD. - whole document but see abstract; page 31, line 30 - page 32, line 22, and Figure 5.	1 - 3, 9, 12, 13, 16, 18, 21
X	WO 98/40809 A2	CHA! TECHNOLOGIES, INC. - whole document but see abstract.	1, 16 at least.
X	"Building a Foundation of Trust in the PC", The Trusted Computing Platform Alliance, January 2000 (located at Internet address: www.trustedpc.org/home/home.htm; see in particular pages 5 and 6).		1, 16 at least

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.